TAKING THE SHACKLES OFF OPERATIONAL INTELLIGENCE TO TACKLE THE NEW RESILIENCE PARADIGM IN FINANCIAL SERVICES

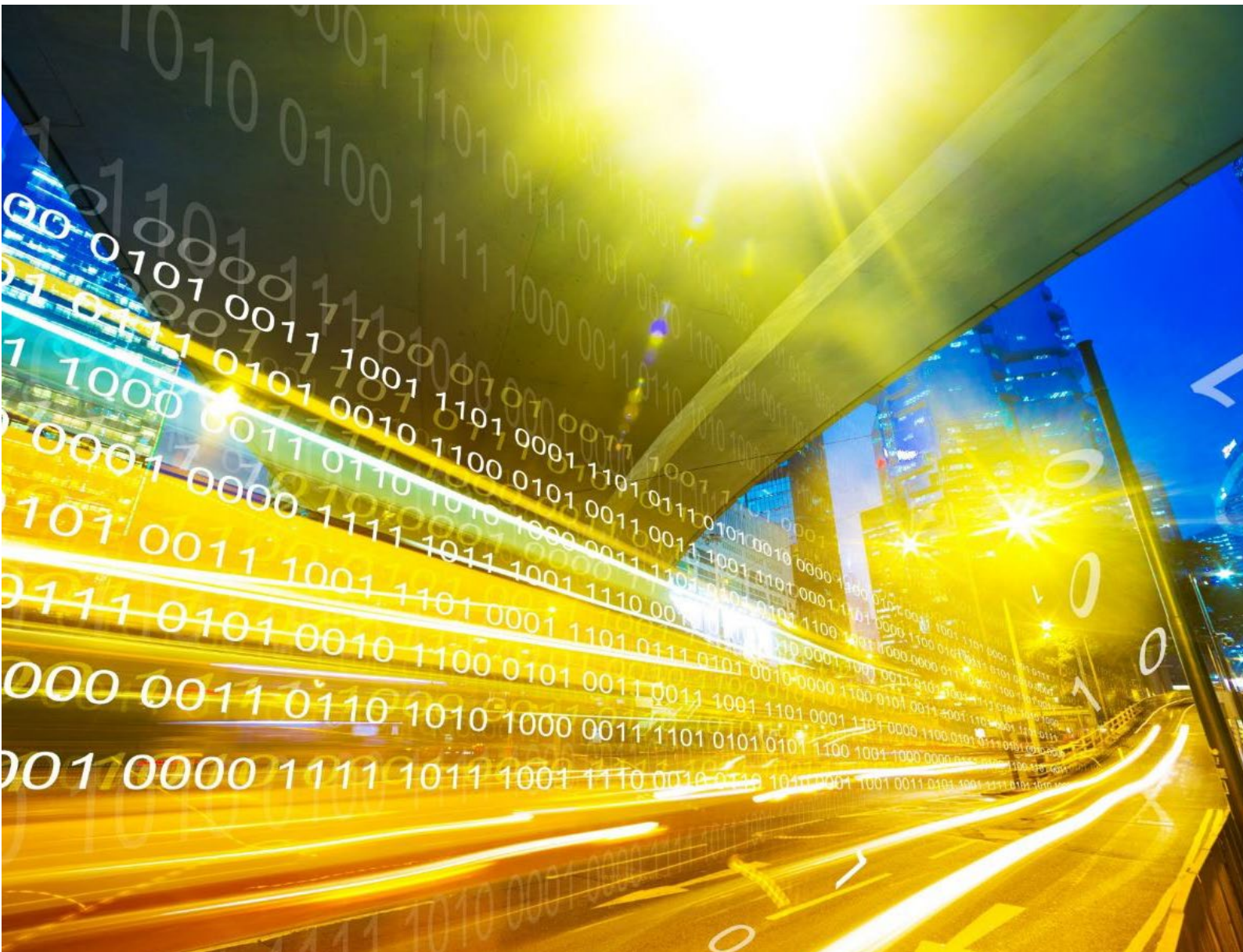
Author:

Tom Zink

September 2022

An IDC Analyst Connection sponsored by ScienceLogic

IDC #EUR149630322



Taking the Shackles Off Operational Intelligence to Tackle the New Resilience Paradigm in Financial Services

Questions posed by: ScienceLogic

Answers by: Tom Zink, Research Director

Q: New regulations, volatility everywhere, and exploding costs keep financial institutions on their toes. Why is AI-based operational intelligence such a major opportunity or even necessity for banking, financial services, and insurance (BFSI) to get a grip on operational resilience?

Since I started covering the financial services industry over 15 years ago, many of the challenges have remained the same. The main culprit is legacy IT. This means a persistent struggle with disconnected and fragmented systems, data silos, and complex IT architectures; rigid processes with manual handoffs causing efficiency bottlenecks, as well as too many data formats and a lack of standards. To make matters worse, a deepening scarcity of talent to maintain these aging systems is forcing BFSI to move or rely on partners and the ecosystem to find solutions to counter the frequent outages and growing cyber risks.

Dissecting how BFSI deals with IT issues shows that it takes too long to identify the root causes of a problem, its impact, and potential dependencies. As many organizations are moving toward a consumption-based IT strategy, relying on "as-a-service" models, resilience increasingly means focusing on the integrity of services and transparency. As architectures get more diversified, the ability to detect anomalies early and to identify the root cause is becoming essential. This is only going to intensify as the integration with the ecosystem intensifies. This raises the bar for operational intelligence capabilities to monitor, observe, manage, and control a complex ecosystem of internal systems, third-party providers, and partners.

Not surprisingly regulation is also zooming in on operational resilience. A new wave is about to hit the industry. The Basel Committee (BCBS) issued principles on operational resilience in March 2021 focusing on change management and information and communication technologies (IT); in the U.S., the Federal Reserve Board (FRB) released sound practices to strengthen operational resilience (SR 20-24) in November 2020; in the U.K. the new rules issued by the Prudential Regulation Authority (PRA), the Bank of England (BoE), and the Financial Conduct Authority (FCA) on operational resilience went active in March 2022; and in the EU the Digital Operational Resilience Act (DORA) is on its way and is expected to be passed later this year.

Q: Operational intelligence has matured in recent years, from simple dashboards to actionable and even predictive insights. How has technology evolved to usher in the paradigm shift we are seeing today?

There are a couple of trends that are now entering mainstream adoption, but the real value is unlocked as they start to work in tandem to reinforce each other.

- The biggest gamechanger is the rise of AI. Technologies such as machine learning and Big Data analytics are changing the way data is collected, insights are generated, and operations are automated. Organizations are turning data into actionable insights that are more proactive and increasingly more predictive.
- The growing maturity of AI tools and platforms, such as AIOps, which combine Big Data and machine learning to platformize and automate IT operations processes, including event correlation, anomaly detection, and causality determination, is transforming operational intelligence.
- The focus is shifting from mere uptime of devices and applications to the integrity of individual business services. In the case of an issue, it is crucial to identify which services are affected and what dependencies are at risk. This helps organizations to prioritize and protect mission-critical services. We see a transformation from performance management to experience management in IT operations.

Integrating multiple separate, manual IT operations tools into a single, intelligent, and automated IT operations platform enables IT operations teams to respond more quickly — even proactively — to slowdowns and outages, with end-to-end visibility and context.

Q: Operational resilience is now also receiving more regulatory attention. How will new regulations, such as DORA, impact this trend?

Operational resilience has become a key priority for regulators around the world, as they grow impatient about frequent IT outages and the ever-increasing threat of cyberattacks. These new regulations also acknowledge the growing importance of a resilient finance ecosystem as third parties such as cloud providers and fintechs take on a critical role in the provision of financial services. The European DORA regulation is probably the most far-reaching initiative, but essentially all regulations are going in a similar direction. The DORA proposal aims to set a worldwide standard when it comes to the operational resilience of the financial sector and oversight of IT providers servicing the sector and will likely be followed by other jurisdictions.

DORA aims to harmonize and expand existing resilience frameworks in the sector. It focuses on the entire IT ecosystem by addressing governance, IT risk management, IT-related incident reporting, digital operational resilience testing, information sharing, and IT third-party risks, including bringing critical IT third-party service providers under the oversight of the European supervisory authorities.

In particular the IT risk management domain builds on operational intelligence to identify, classify, and document all business-critical IT functions, information assets, and

interdependencies between internal and external IT systems. It mandates the implementation of IT security strategies, policies, procedures, and tools to ensure resilience and availability of IT systems as well as the security, confidentiality, and integrity of data. BFSI must have in place alert mechanisms to detect anomalous activities and incidents.

But DORA goes further as it evolves existing requirements to continuously improve capabilities such as analyzing the cause of IT incidents and identifying necessary improvements, as well as implementing the learnings from digital operation resilience testing and generally improving IT security awareness and digital operational resilience training.

Current expectations are that DORA will become law in late 2022 or early 2023, but it will not have to be implemented for another 12 to 24 months.

Q: What's the vision for operational intelligence? Are we moving toward self-healing operations or autonomous operations?

The future is clearly going in this direction, but we still have some way to go before we can call it self-healing or autonomous operations. Having said that, this is already starting for simpler and recurring issues, where intelligent automation can execute or replicate a response. While humans are still the main decision maker, the execution is more and more automated.

Another major shift is that the decisions are taken by business users or operations staff instead of IT. As faster "time to recovery" becomes a key objective, the ability to put operations staff and even business users into the driver's seat by empowering them to understand and resolve the issue by themselves will be key to take operational resilience to the next level.

To make this work, three underlying capabilities are necessary:

- The ability to collect data natively across a heterogenous estate of source systems as close to real time as possible
- The analytics capabilities and infrastructure to turn Big Data into actionable insights
- Automation capabilities to generate recommendations for employees or even execute resolution measures autonomously

MESSAGE FROM THE SPONSOR

ScienceLogic is a leader in IT operations management, providing modern IT operations with actionable insights to predict and resolve problems faster in a digital, ephemeral world. Its IT infrastructure monitoring and AIOps platform sees everything across cloud and distributed architectures, contextualizes data through relationship mapping, and acts on this insight through integration and automation. Trusted by thousands of organizations, ScienceLogic's technology was designed for the rigorous security requirements of the U.S. Department of Defense, proven for scale by the world's largest service providers, and optimized for the needs of large enterprises.

Organizations continue to adopt AIOps to deliver better digital experiences for employees, remote operations teams, and customers as they undergo large-scale digital transformation. ScienceLogic helps IT operations executives significantly improve their customer experience through faster mean time to repair (MTTR), utilizing high levels of automation to drive down costs. ScienceLogic's clients include Cisco (which reduced MTTR by 97%), Southwest Airlines (which replaced 28 tools with ScienceLogic), and NetDesign (which saved $1.5 million and reduced SLA breaching incidents by 60%).

Investing in AIOps requires strategic planning and a strong business case. Explore and build the business case for your AIOps journey with the AIOps Value Calculator.

About the Analyst

Tom Zink, Research Director, IDC Financial Insights

Tom Zink leads IDC's European financial services research. He has covered the financial services industry as an analyst and journalist for the past 15 years, and his core focus areas are corporate banking and ecosystem banking strategies.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.uk.idc.com

Global Headquarters

140 Kendrick Street,
Building B
Needham,
MA 02494
+1.508.872.8200
www.idc.com

Copyright and Restrictions